

REMARKS

In the Office Action, the "Examiner rejected Claims 1-17, which were all of the then pending claims, under 35 U.S.C. 103 as being unpatentable over the prior art, principally, WO 01/59545 (Subramanian). In particular, Claims 1, 3-5 and 7-17 were rejected as being unpatentable over Subramanian in view of U.S. Patent 5,870,473 (Boesch, et al.). Claim 2 was rejected as being unpatentable over Subramanian and Boesch, et al. in view of WO 00/01108 (McLaughlin), and Claim 6 was rejected as being unpatentable over Subramanian and Boesch, et al in view of U.S. Patent 5,794,207 (Walker, et al.).

Independent Claims 1, 13 and 17 are being amended to better define the subject matters of these claims. New Claim 18, which is dependent from Claim 1, is being added to describe a preferred feature of the invention.

For the reasons discussed below, Claims 1-18 patentably distinguish over the prior art and are allowable. The Examiner is thus asked to reconsider and to withdraw the rejections of Claims 1-17 over the prior art, and to allow these claims and new Claim 18.

Generally, Claims 1-18 patentably distinguish over the prior art because the prior art does not disclose or suggest using a trusted body to record a dialogue by encrypting each message of the dialogue using a public key of a private key/public key pair, as described in independent Claims 1, 13 and 17.

To elaborate, the present invention, generally, relates to communications between at least two parties in a dialogue via a computer network. As discussed in the instant application, the advent of the Internet and other computer networks has resulted in the development of new forms of communication. One popular new form is the "chat room," where users communicate with each other. In chat rooms, however, there is no assurance that

what is said is accurate or reliable, and it is difficult or impossible to verify that a particular person made any particular statement. Thus, chat rooms are not suitable for many types of dialogues such as business negotiations.

This invention addresses this issue. In particular, the invention provides a method and system for facilitating dialogue between two or more parties via a computer network, such as the Internet, which provides anonymity, accountability, and agrees set of rules for the dialogue. In accordance with the preferred embodiment of the invention, a plurality of users registers with a trusted body. That trusted body verifies the identity of each user, generates a random identifier for each user, and keeps a confidential record of the relation between the identity of each user and the random identifier for that user.

One of the users enters into a dialogue with one or more other users by sending messages over the computer network and through the trusted body to said one or more other users. Each user is able to remain anonymous through use of its random identifier until such time as the user reveals its identify to one or more of the other users. Also, the trusted body records the dialogue by encrypting each message of the dialogue using a public key of a private key/public key pair of the trusted body; and the trusted body then uses the recorded dialogue, together with the confidential record of the relation between the identity of a user and the random identifier, to provide a means to verify the dialogue by the users. Specifically, a user cannot effectively deny that he or she sent a particular message because all messages are sent through the trusted body, and that body records all those messages.

The references of record do not disclose or suggest this type of use of the trusted body – that is, using the trusted body to record each message of the dialogue by using the public key of a private key/public key pair of that trusted body.

For instance, Subramaniam describes a procedure for providing anonymous Internet transactions. In this procedure, an agent monitors and maintains the anonymity of transactions between two registered users on a secure computer system. After a user registers an account, the secure system permits the user to view and to post messages on the system. Each messages posted to the system passes through the agent to prevent the inadvertent disclosure of identifying information by warning the user of the disclosure and requiring the user to authorize the disclosure before posting the message. Also, in the system disclosed in Subramaniam, each party may instruct the agent to permit the disclosure of identifying information.

There is an important, general difference between the present invention and the method and system disclosed in Subramaniam. In particular, the present invention is directed to enabling effective, subsequent verification of a complete dialogue, while Subramaniam is not specifically directed to this same issue.

This general difference between the present invention and the procedure disclosed in Subramaniam is reflected in a number of more specific differences. For example, with the instant invention, the trusted body records each message and encrypts each message using the public key of a private key/public key pair. This allows the trusted body – and only that body – to later decrypt the stored message using the private key of this key pair. Due to this, if the trusted body later sends the messages back to the users, those users can be assured that the message is the message that was sent to and stored by the trusted body.

Independent Claims 1, 13 and 17 are being amended to describe the above-discussed feature of the present invention. In particular, both of these claims are being amended to

indicate that the trusted body, among other functions, encrypts each message of the dialogue using a public key of a public key pair of the trusted body.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest this feature of the invention.

For example, Boesch, et al. discloses a procedure for conducting economic transactions in a secure manner over insecure networks such as the Internet. Boesch, et al. is thus directed to security, not to verifying what was said between the parties. Boesch, et al. was cited by the Examiner for its disclosure of generating a user identifier that is a random number. The procedure described in Boesch, et al. does not need to encrypt each received message, and clearly does not use the public key of a private/public key pair to do this.

McLaughlin discloses a system and method for processing bi-directional, anonymous or pseudo-anonymous user transactions. In this method, a number of digital certificates are created, and a plurality of operating modules is provided to perform various tasks. In normal operation, no one module within the system possesses enough information to determine the user's confidential identity and to connect the user to a particular transaction or to a particular anonymous or pseudo-anonymous identity.

Walker was cited by the Examiner for its disclosure of time stamping messages of a dialogue. This reference describes a buyer-seller protocol, in which a trusted third party may be used to determine fulfillment, adequacy and interpretation of a contract or contract offer.


The procedures disclosed in McLaughlin-Walker also have no need to record each message in the manner that each message is recorded by the trusted body in accordance with the present invention.

In view of the above-discussed differences between Claims 1, 13 and 17 and the prior art, and because of the advantages associated with those differences, Claims 1, 13 and 17 patentably distinguish over the prior art and are allowable. Claims 2-12 and 18 are dependent from Claim 1 and are allowable therewith. Similarly, Claims 14-16 are dependent from, and are allowable with, Claim 13.

The Examiner is, accordingly, respectfully requested to reconsider and to withdraw the rejections of Claims 1-17 under 35 U.S.C. 103, and to allow these claims and new Claim 18.

If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,


John S. Sensny
Registration No. 28,757
Attorney for Applicant

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 7472-4343

LP:jy